Remarks/Arguments

Claims 1-5, and 7-22 are pending. Claim 6 has been cancelled herein. Independent Claims 21 and 22 have been newly added. New Claim 22 incorporates the subject matter of now cancelled Claim 6, and the base and intervening claims from which Claim 6 depends. Accordingly, Applicants respectfully submit Claim 22, and Claims 7 – 9, which depend from Claim 22, are in condition for allowance, early notification of which is earnestly solicited. New Claim 21 incorporates the subject matter of now cancelled Claim 6 and Claim 1, the base claim upon which now cancelled Claim 6 ultimately depended. Applicants respectfully submit Claim 21 is similarly in condition for allowance, early notification of which is also earnestly solicited.

Applicants acknowledge withdrawal of the finality of the last Office action and withdrawal of the previous rejection(s) under 35 USC 103(a). Applicants further acknowledge Examiner's indication of allowable subject matter defined in claims 6-10.

1. 35 U.S.C. 112, First Paragraph Rejections

The Examiner asserts on pages 2-3 of the present Office action

> "Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for a method for managing access between a service provider and a set-top box having a smart card coupled thereto (applicant's specification, pgs. 5-12), ***does not reasonably provide enablement for a method for managing access to a device***. The specification does not enable any person skilled in the art...to make or use the invention commensurate in scope with these claims. ***The claimed invention is much broader than the enabling portion of the specification; for example, the specification does not enable a method for managing access to non-set top boxes***, such as hand held palms or mobile phones, or in transactions between computing devices incorporating other secure protocols such as IPsec". (*emphasis added*)

Applicants respectfully traverse this rejection. MPEP 2164.08 states "[w]hen analyzing the enables scope of a claim, the teachings of the specification must not be ignored because claims are to be given their broadest reasonable interpretation

that is consistent with the specification." Applicants submit that the subject matter of the present claims is supported and enabled by the specification as filed. By way of example, Applicants' specification on page 1, line 5 – page 2, line 6 states

> *"This invention concerns a system for providing conditional access (i.e., managing access) to a device, such as a "consumer electronic device". Examples of such consumer electronic devices include separate devices or "boxes" that may be located on top of, and coupled to a television receiver, i.e., set-top boxes."*

In addition to the above disclosure, Applicants' specification further states on page 1, lines 15-18 that

> "*Conditional access may be achieved by connecting two devices together when communication therebetween is desired and by disconnecting the devices from one another when communication is no longer desired."*

Still further, page 12, lines 20-22 of the specification states

> *"...it is within the scope of the present invention that the conditional access system defined herein is fully capable of being utilized between any two devices interconnected."*

The above passages illustrate that the scope of Claims 1 – 10 is not impermissibly broad, but rather is commensurate with the enabling portions of the specification. As indicated above, the specification expressly recites that the present invention is applicable to devices such as consumer electronic devices, and provides set-top boxes as an *example* of such electronic devices. The summary of the invention and detailed description of the drawings likewise support the breadth of the claimed invention, and articulate the applicability of the conditional access system to any two interconnected devices. While the application describes exemplary implementations within the context of a set-top box having a smart card coupled thereto, a service provider and associated server, Applicants submit the claimed invention need not be limited to that specific embodiment and detailed technological device(s) recited therein, as suggested in the present Office action. *"That claims are interpreted in light of the specification does not mean that everything in the specification must be read into the claims." Raytheon Co. v. Roper Corp. 724 F2d 951, 957.*

Further yet, Claims 1-5, and 7-10 recite patentable process steps having operability over a broad range of devices suitable for operating with the messages and data recited therein. MPEP 2164.08 further states that *"the specification must teach those skilled in the art how to make and use the full scope of the claimed invention without 'undue experimentation' " and that "the scope of enablement must only bear a 'reasonable correlation' to the scope of the claims."* Applicants respectfully submit that the present disclosure meets the above criteria, as is even acknowledged by the present Office action which rejects Claims 1-10 over an example set forth in the Schneier reference, which fails to even reference set-top boxes.

For the foregoing reasons, Applicants submit that present Claims 1 and 10 are fully supported by the specification as originally filed, which specification enables one of ordinary skill in the art to make and use the claimed invention. Reconsideration and removal of this 35 USC 112 rejection is respectfully requested.

2. 35 U.S.C. 101 Rejections

Claims 1-10 stand rejected under 35 U.S.C. 101. The Office action asserts that the claims are not tangibly embodied "since none of the steps define the use of network hardware to actuate the handshake method" and that the claims are not "tied to a technological art" which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 USC 101.

In response, Applicants have amended Claim 1 to recite "[a] method for managing access to an electronic device...comprising...sending a first message from a first electronic device to a second electronic device...". The method further comprises receiving in the first device a digital certificate from the second device, receiving in the first device the first message encrypted using a second private key of the second device, authenticating the second device, and establishing a communications channel between the first and second devices in response to the authentication. Accordingly, Applicants submit present Claim 1 is not directed to merely an abstract idea, as it clearly and unambiguously recites a patentable process tied to the electronic/computer related technological arts, that includes

sending and receiving messages via electronic devices, performing an authentication using the received messages, and establishing a communications channel upon authentication.

Claim 10 has been amended in similar fashion, and recites sending data, receiving a digital certificate having data, encrypting data, decrypting the certificate, decrypting data, comparing data, sending encrypted data and establishing a communications channel between electronic devices. Accordingly, Applicants submit present Claim 10 also clearly and unambiguously recites a patentable process for managing access to an electronic device, and is not merely directed to an abstract idea.

For purposes of completeness, new claims 21 and 22 recite similar process steps, including sending data, receiving data, authenticating, and establishing a communications channel.

For at least these reasons, Claims 1-10, as well as new claims 21-22, meet the requirements of 35 USC 101; reconsideration and removal of this rejection is requested.

3. 35 U.S.C. 103(a) Rejections

A. Claims 1-5, 11 and 12-20.

Claims 1-5, 11 and 12-20 stand rejected pursuant to 35 U.S.C. 103(a) as being unpatentable over the teachings of Schneier. These rejections are respectfully traversed. 35 U.S.C. 103(a) sets forth in part:

> [a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* Applicants respectfully submit Schneier fails to teach, or suggest, each of the recited limitations

of any of the pending claims, and as a matter of law fails to render any of the present claims unpatentable for at least the following reasons.

(1) Schneier Fails to Teach or Suggest Use of First and Second Private Keys as Recited in Claim 1.

Claim 1 recites, in part:

> A method for managing access to an electronic device, said method comprising:
> (a) sending a first message from a first electronic device to a second electronic device;
> (b) receiving, in said first device, from said second device a digital certificate encrypted using *a first private key of said second device*;
> (c) receiving, in said first device, from said second device said first message encrypted using *a second private key of said second device*. (*Emphasis added*)

Schneier fails to teach, or suggest, the claimed use of a digital certificate encrypted using a first private key of the second device, and a first message encrypted using a second private key of said second device. In the example of Schneier on page 54 that is referenced in the Office action, Alice uses only a single private key to encrypt a random string and send it back to the host. Modifying the teachings of this example to use a digital certificate to certify a public key fails to remedy the shortcoming of the example in Schneier, because Schneier still fails to teach or suggest the use of first and second private keys associated with the recited second electronic device. For at least this reason, Applicants submit the referenced portions of Schneier fail to teach or suggest each of the limitations of present Claim 1 – and hence, as a matter of law Claim 1 is patentably distinguishable over Schneier.

More particularly, the Office action argues Schneier's teaching of a host sending Alice a random string, Alice encrypting that string using her private key, and transmitting it back to the host, corresponds to the Claim 1 recitation of "(a) sending a first message from a first device to a second device; ... [and] (c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device." *See, 3/31/2005 Office action, pars. 9a and 9b.* The Office action goes on to acknowledge the referenced Schneier scheme fails to

teach digital certificates – no less a digital certificate encrypted using a private key different from that used to encrypt the host's random string. *See, 3/31/2005 Office action, par. 10.*

To remedy this admitted shortcoming, the Office action attempts to import the teachings of Schneier with regard to certificates on pages 574-576. *See, 3/31/2005 Office action, par. 10 (paying particular attention to the 3rd full paragraph).* Relying on the above passage, the Office action concludes:

> Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a digital certificate to certify a public key, wherein prior to using the certified public key, the digital certificate is authenticated using a public key to verify the signature on the digital certificate since it certifies a specific public key with a specific user. *3/31/2005 Office action, par. 10.*

In response, Applicants submit that a detailed reading of Schneier reveals that, even assuming arguendo that the separate teachings within Schneier can be combined as suggested by the Examiner, modifying the example on page 54 of Schneier to use a digital certificate to certify a public key still fails to teach or suggest the claimed use of first and second private keys associated with the recited second device. The Office action itself argues a public key stored in a certificate is used for cryptographic processing once validated. *See, 3/31/2005 Office action, par. 10.* The Office action goes on to argue that the certificate requires a first private key to sign it. *See, 3/31/2005 Office action, par. 10.* In contradistinction to the claimed invention, the certificate is signed with the certificate authority's private key, such that anyone possessing the certificate authority's public key may authenticate the certificate as being valid. *See, e.g., Schneier, page 575, lines 14-15 ("The last line is the CAs signature.")* Modifying the example on page 54 of Schneier such that the host uses a certificate to acquire a certified public key, instead of merely looking one up in its database, does not teach the claim limitation of first and second private keys associated with the second party as recited in present Claim 1. The key used to sign the certificate is merely a private key associated with the certificate authority and not the certificate holder.

Accordingly, the Schneier reference fails to teach or suggest each of the features and limitations recited in present Claim 1; reconsideration and withdrawal of

this 35 USC 103 rejection is respectfully requested. Applicants also respectfully request reconsideration and removal of the rejections of Claims 2–5 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.

(2) The Cited Art Fails to Teach or Suggest the Use of First and Second Private Keys as Recited in Claims 11-20.

Claim 11 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Ohashi. Claims 12–20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Ohashi, and further in view of Force. Applicants respectfully traverse these rejections for at least the following reasons.

The arguments discussed above with respect to present Claim 1 in view of Schneier also apply to present Claim 11. Claim 11 recites in relevant part a method for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

> (e) receiving from the service provider, in response to said second message, *a second digital certificate encrypted using a second private key of said service provider*; [and]
> (f) receiving from the service provider said *second message encrypted using a third private key*.

Such features and limitations are neither taught nor suggest by the prior art of record. Accordingly, Applicants respectfully submit Schneier fails to teach or suggest each of the limitations recited in Claim 11. Ohashi is cited as disclosing a method for authenticating a cryptographic link between a service provider and a client terminal using a smart card coupled thereto by means of certificate authentication. Even if Ohashi teaches such a features, applicants submit that Ohashi fails to cure the defect of Schneier as applied to the limitations cited above as discussed hereinabove. Reconsideration and removal of this 35 USC 103 rejection of Claim 11 is respectfully requested.

Force is cited as disclosing a smart card designed to incorporate multiple types of information, including a plurality of certificates, each certificate identifying a distinct service. Even if Force teaches such a feature, Applicants submit that the reference of Force also fails to add anything to the combined teachings of Schneier and Ohashi in regards to Claims 12-20. Accordingly, Applicants also request

reconsideration and removal of the 35 USC 103 rejection of Claims 12-20 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 11.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding remarks, this application stands in condition for allowance. Reconsideration and allowance of this application is respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicants' attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

Ahmet M. Eskicioglu, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312
Date: July 25, 2005

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

JULY 25, 2005
Date

Linda Tindall
Linda Tindall